The System Safety Society

Tennessee Valley Chapter

Professionals Dedicated to the Safety of Systems, Products and Services

Greetings to all competitors entering the 2009 running of The Great Moonbuggy Race!
This year, the Tennessee Valley Chapter of the international System Safety Society is working with organizers of The Great Moonbuggy Race to judge and present the **System Safety Challenge**. Two trophies will be awarded – one to the college team and one to the high school team – for the best application of System Safety Engineering.

System Safety is a formal discipline characterized by the application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout the system life cycle. System Safety has evolved as a distinct engineering discipline in the post-WWII era of increasingly complex systems whose accident risks are less and less tolerable to society. System Safety has been effectively applied in a wide variety of industries and programs, including space flight, military weapons, transportation, energy, and chemical processing, to name but a few. More information on System Safety is readily available on a variety of Internet sites, including the System Safety Society's website, http://mail.system-safety.org/

System Safety is most effective and economical when begun as early in system development as possible – before details of the design are firm and when there is the most opportunity to influence the design. Safety needs to be *designed in*, rather than added as an afterthought. One of the most important System Safety activities is the *hazard analysis*. A *hazard* is any real or potential condition that can result in death, injury, or illness to personnel; damage to or loss of equipment or property; or damage to the environment. In a hazard analysis, the analyst identifies and characterizes the credible hazards posed by the system or its operation, assesses the risk associated with each hazard (in terms of *severity* of consequences and *probability* of occurrence), and identifies real or proposed means for eliminating the hazard or minimizing its risk. Results of the hazard analysis are usually compiled in a series of hazard reports or hazard logs, giving a thorough characterization of each hazard. These hazard data are used by the project team to manage risks and incorporate hazard control measures in a prioritized fashion.

The preferred order for controlling hazards is (1) eliminate the hazard by designing it out, (2) implement safety devices such as guards, interlocks, or redundant systems, (3) provide warning devices such as lights, alarms, displays, or signs, and (4) institute special procedures or training.

Participants in The Great Moonbuggy Race may enter the **System Safety Challenge** by submitting a documentation package, in a format of their choosing, following the submittal instructions on the attached sheet. In addition to stating where and how your package should be submitted, the attached sheet also provides a suggested content outline and judging criteria.
Entries in the **System Safety Challenge** must be received by 5:00 PM CST on March 18th, 2009
NOTE: Please get a receipt for your application from Jim Blanteno. Good luck to all participants!

The System Safety Challenge

- An optional award offered as part of The Great Moonbuggy Race, 2009

• **Submission Instructions**

Entries must be submitted electronically, by U.S. Mail, or by other delivery service to Jim Blanteno with conformation requested. Entries submitted to anyone else will not be considered.

James Blanteno
A-P-T Research
4950 Research Drive
Huntsville, AL 35805
256-313-2090
James.Blanteno@redstone.army.mil

Entries must be received by 5:00 CST on March 18th, 2009.

• **Submission Guidelines**

To ensure the judges are able to fully evaluate your submittal, the following content is suggested:
- A preliminary hazard list (PHL), identifying the general hazard types expected to be identified by analysis
- Safety-related requirements that you determine, in advance, should be met by your system; explain how these requirements flow to the design implementation
- A hazard analysis report, which should
- Bound and describe your system, including its safety critical functions
- Explain how your hazard analysis was conducted
- Define terms, including any used to characterize hazards or safety risks posed
- State assumptions and/or limitations
- Document hazard data generated by analysis (no more than 10 hazard logs)
- Identify design features that eliminate or control hazards or result in a robust Design

• **Judging Criteria**

The judges' decisions are final. A panel of judges from the Tennessee Valley Chapter of the System Safety Society will evaluate each participant's understanding and application of System Safety based on the following:
- Thoroughness, clarity, credibility, and organization of hazard identification results as documented in the PHL and hazard logs
- Description of safety critical functions
- Adequacy and appropriate application of design features to eliminate or control hazards or result in a robust design
- Traceability of safety-related requirements to design implementation